

ON THE NON-EXISTENCE OF SHARPLY TRANSITIVE SETS OF PERMUTATIONS IN CERTAIN FINITE PERMUTATION GROUPS

PETER MÜLLER AND GÁBOR P. NAGY

ABSTRACT. In this short note we present a simple combinatorial trick which can be effectively applied to show the non-existence of sharply transitive sets of permutations in certain finite permutation groups.

1. INTRODUCTION

A permutation code (or array) of length n and distance d is a set S of permutations of some fixed set Ω of n symbols such that the Hamming distance between each distinct $x, y \in S$ is at least d , see [3]. By elementary counting, one has $|S| \leq n(n-1) \cdots d$ and equality holds if and only if S for any two tuples $(x_1, \dots, x_{n-d+1}), (y_1, \dots, y_{n-d+1})$ of distinct symbols, there is a unique element $s \in S$ with $x_1^s = y_1, \dots, x_{n-d+1}^s = y_{n-d+1}$. Such sets of permutations are called *sharply t -transitive*, where $t = n - d + 1$. It is well known that sharply 1- and 2-transitive sets of permutations correspond to Latin squares and affine planes, respectively [2].

In general, there are very few results on permutation codes and there is a large gap between the lower and upper estimates for $|S|$; see [9], [8]. Most of the known constructions are related to multiply transitive permutation groups. In the 1970's, P. Lorimer started the systematic investigation of the question of existence of sharply 2-transitive sets in finite 2-transitive permutation groups. This program was continued by Th. Grundhöfer, M. E. O'Nan, P. Müller, see [6] and the references therein. Some of the 2-transitive permutation groups needed rather elaborated methods from character theory in order to show that they do not contain sharply 2-transitive sets of permutations.

In this paper, we present some simple combinatorial methods which are useful to exclude the existence of sharply 1- and 2-transitive sets of permutations in given finite permutation groups.

Notice that if S is a sharply t -transitive set of permutations on Ω , then it is also a sharply 1-transitive set of permutations on the set $\Omega^{(t)}$ of t -arrangements of Ω . In other words, the t -transitive permutation

The second author was supported by DAAD and TAMOP project 4.2.2-08/1/2008-0008.

group G contains a sharply t -transitive set if and only if in its induced action on $\Omega^{(t)}$, G contains a sharply 1-transitive set.

Let G be a permutation group on the set $\Omega = \{\omega_1, \dots, \omega_n\}$ and for $g \in G$, denote by $\pi(g)$ the corresponding permutation matrix. Let J denote the $n \times n$ all-one matrix. The existence of sharply transitive sets in G is equivalent to the $\{0, 1\}$ -solvability of the matrix equation

$$(1) \quad \sum_{g \in G} x_g \pi(g) = J.$$

For some permutation groups we are able to show that (1) has no integer solution, which implies the nonexistence of a sharply transitive set in the given group.

2. CONTRADICTING SUBSETS

The following simple lemma will be our main tool.

Lemma 1. *Let S be a sharply transitive set of permutations on a finite set Ω . Let B and C be arbitrary subsets of Ω . Then $\sum_{g \in S} |B \cap C^g| = |B||C|$.*

Proof. Count the set of triples (b, c, g) , where $b \in B$, $c \in C$, $g \in S$ and $c^g = b$, in two ways: If b, c is given, then there is a unique g by sharp transitivity. If g is given, then the number of pairs b, c is $|B \cap C^g|$. \square

An immediate consequence is

Lemma 2. *Let G be a permutation group on a finite set Ω . Assume that there are subsets B, C of Ω and a prime p such that $p \nmid |B||C|$ and $p \mid |B \cap C^g|$ for all $g \in G$. Then G contains no sharply transitive set of permutations.*

Remark. It is easy to see that under the assumption of Lemma 2, the system (1) does not have a solution in the finite field \mathbb{F}_p , so in particular (1) has no integral solution.

We give several applications of these lemmas. First, we show that in even characteristic, the symplectic group does not contain sharply transitive sets of permutations.

Theorem 3. *Let n, m be positive integers, $n \geq 2$, $q = 2^m$. Let $G_1 = PSp(2n, q) \rtimes \text{Aut}(\mathbb{F}_q)$ and $G_2 = Sp(2n, q) \rtimes \text{Aut}(\mathbb{F}_q)$ be permutation groups in their natural permutation actions on $\Omega_1 = PG(2n-1, q)$ and $\Omega_2 = \mathbb{F}_q^{2n} \setminus \{0\}$. Then, G_1 and G_2 do not contain a sharply transitive set of permutations.*

Proof. We deal first with the projective group G_1 . Let \mathcal{E} be an elliptic quadric whose quadratic equation polarizes to the invariant symplectic form $\langle \cdot, \cdot \rangle$ of G_1 . Let ℓ be a line of $PG(2n-1, q)$ which is nonsingular with respect to $\langle \cdot, \cdot \rangle$. Then for any $g \in G_1$, ℓ^g is nonsingular, that is,

it is not tangent to \mathcal{E} . In particular, $|\mathcal{E} \cap \ell^g| = 0$ or 2 for all $g \in G_1$. Furthermore, we have

$$|\mathcal{E}| = \frac{q^{2n-1} - 1}{q - 1} - q^{n-1}, \quad |\ell| = q + 1,$$

both odd for $n \geq 2$. We apply Lemma 2 with $B = \mathcal{E}$, $C = \ell$ and $p = 2$ to obtain the result of the theorem.

In order to show the result for the group G_2 , we define the subsets $\mathcal{E}' = \varphi^{-1}(\mathcal{E})$ and $\ell' = \varphi^{-1}(\ell)$, where $\varphi : \Omega_2 \rightarrow \Omega_1$ is the natural surjective map. Then,

$$|\mathcal{E}'| = (q - 1)|\mathcal{E}|, |\ell'| = (q - 1)|\ell| \text{ and } |\mathcal{E}' \cap \ell'| \in \{0, 2(q - 1)\}.$$

Hence, Lemma 2 can be applied with $B = \mathcal{E}'$, $C = \ell'$ and $p = 2$. \square

It was a long standing open problem whether the Mathieu group M_{22} contains a sharply transitive set of permutations, cf. [5]. The negative answer given in the following theorem implies the nonexistence of sharply 2-transitive sets in the Mathieu group M_{23} .

We will use the Witt design \mathcal{W}_{23} . This is a $(23, 7, 4)$ -Steiner system. The fact which we use here and again in the proof of Theorem 7 is that any two blocks of \mathcal{W}_{23} intersect in 1, 3, or 7 points.

Theorem 4. *In its natural permutation representation of degree 22, the Mathieu group M_{22} does not contain a sharply transitive set of permutations.*

Proof. Let $\Omega' = \{1, \dots, 23\}$, $\Omega = \{1, \dots, 22\}$ and $G = M_{22}$ be the stabilizer of $23 \in \Omega'$. Let $B \subset \Omega$ be a block of the Witt design \mathcal{W}_{23} , and $C = \Omega \setminus B$. Then, $|B| = 7$, $|C| = 15$ and for all $g \in G$, $|B \cap C^g| = 0, 4$ or 6 . Lemma 2 implies the result with $p = 2$. \square

We can apply our method for certain alternating groups, as well. The following simple result is somewhat surprising because until now, the symmetric and alternating groups seemed to be out of scope in this problem.

Theorem 5. *If $n \equiv 2, 3 \pmod{4}$ then the alternating group A_n does not contain a sharply 2-transitive set of permutations.*

Proof. Assume $n \equiv 2, 3 \pmod{4}$ and let G be the permutation action of A_n on the set $\Omega^{(2)}$ with $\Omega = \{1, \dots, n\}$. A sharply 2-transitive set of permutations in A_n corresponds to a sharply transitive set of permutations in G . Define the subsets

$$B = \{(x, y) \mid x < y\}, \quad C = \{(x, y) \mid x > y\}$$

of $\Omega^{(2)}$. By the assumption on n , $|B| = |C| = n(n - 1)/2$ is odd. For any permutation $g \in S_n$, we have

$$|\{(x, y) \mid x < y, x^g > y^g\}| \equiv \text{sgn}(g) \pmod{2}.$$

This implies $|B \cap C^g| \equiv 0 \pmod{2}$ for all $g \in A_n$. Thus, we can apply Lemma 2 to obtain the nonexistence of sharply transitive sets in G and sharply 2-transitive sets in A_n . \square

Theorems 4 and 5 can be used to prove the nonexistence of sharply 2-transitive sets in the Mathieu group M_{23} .

Corollary 6. *In its natural permutation representation of degree 23, the Mathieu group M_{23} does not contain a sharply 2-transitive set of permutations.*

As the last application of our contradicting subset method, we deal with the stabilizer of the sporadic group Co_3 in its doubly transitive action on 276 points. As a corollary, we obtain a purely combinatorial proof for a theorem by Grundhöfer and Müller saying that Co_3 has no sharply 2-transitive set of permutations. Notice that the original proof used the Atlas of Brauer characters.

Theorem 7. *Let G be the group $McL:2$ in its primitive permutation action on 275 points. Then, G does not contain a sharply transitive set of permutations.*

Proof. Identify G with the automorphism group of the McLaughlin graph Γ , acting on the 275 vertices. We claim that there are subsets B and C of vertices with $|B| = 22$, $|C| = 56$, and $|B \cap C^g| \in \{0, 3, 6, 12\}$ for all $g \in G$. The theorem then follows from Lemma 2 with $p = 3$.

In order to describe B and C , we use the construction of Γ based on the Witt design \mathcal{W}_{23} , see e.g. [1, 11.4.H]. Let $B \cup \{q\}$ be the 23 points of \mathcal{W}_{23} . Let U be the 77 blocks of \mathcal{W}_{23} which contain q , and V be the 176 blocks which do not contain q . The vertices of Γ are the $22 + 76 + 176 = 275$ elements from $B \cup U \cup V$. Adjacency \sim on Γ is defined as follows: The elements in B are pairwise non-adjacent. Furthermore, for $b \in B$, $u, u' \in U$, $v, v' \in V$ define: $b \sim u$ if $b \notin u$, $b \sim v$ if $b \in v$, $u \sim u'$ if $|u \cap u'| = 1$ (so $u \cap u' = \{q\}$), $v \sim v'$ if $|v \cap v'| = 1$, and $u \sim v$ if $|u \cap v| = 3$.

This construction gives the strongly regular graph Γ with parameters $(275, 112, 30, 56)$. Pick two vertices $i \neq j$ which are not adjacent, and let C be the set of vertices which are adjacent to i and j . Then $|C| = 56$. For $g \in G = \text{Aut}(\Gamma)$, C^g is again the common neighborhood of two non-adjacent vertices. Thus without loss of generality we may assume $g = 1$, so we need to show that $|B \cap C| = 0, 3, 6$, or 12 . Suppose that $|B \cap C| > 0$. Then there is a vertex $x \in B \cap C$ which is adjacent to i and j . Therefore $i, j \notin B$. Recall that two distinct blocks of \mathcal{W}_{23} intersect in either 1 or 3 points.

We have to consider three cases: First $i, j \in U$. Then $|i \cap j| = 3$ and $q \in i \cap j$. Furthermore, $B \cap C = B \setminus (i \cup j)$, so $|B \cap C| = 12$. Next, if $i, j \in V$, then $|i \cap j| = 3$ and $B \cap C = i \cap j$, so $|B \cap C| = 3$. Finally, if

$i \in U, j \in V$, then $|i \cap j| = 1$ and $B \cap C = j \setminus i$, so $|B \cap C| = 6$ and we have covered all cases. \square

3. ON 2-TRANSITIVE SYMMETRIC DESIGNS

As another application of the lemma we reprove [6, Theorem 1.10] without using character theory. In particular, Lorimer's and O'Nan's results [7] about the nonexistence of sharply 2-transitive sets of permutations in $\text{P}\Gamma\text{L}_k(q)$ ($k \geq 3$) hold by simple counting arguments.

Theorem 8. *Let G be an automorphism group of a nontrivial symmetric design. Then the stabilizer in G of a point does not contain a subset which is sharply transitive on the remaining points. In particular, G does not contain a subset which is sharply 2-transitive on the points of the design.*

Proof. Let $v > k > \lambda$ be the usual parameters of the design. So the set Ω' of points of the design has size v , each block has size k , and two distinct blocks intersect in λ point. We will use the easy relation $(v - 1)\lambda = k^2 - k$ (see any book on designs).

Fix $\omega \in \Omega'$, let G_ω be the stabilizer of ω in G , and suppose that $S \subseteq G_\omega$ is sharply transitive on the set $\Omega := \Omega' \setminus \{\omega\}$ of size $v - 1$. As each point is contained in $k < v$ blocks, there is a block B with $\omega \notin B$. Apply Lemma 1 with $C = B$, so

$$\sum_{g \in S} |B \cap B^g| = |B|^2 = k^2.$$

Let a be the number of $g \in S$ with $B = B^g$. In the remaining $|S| - a = v - 1 - a$ cases we have $B \neq B^g$, hence $|B \cap B^g| = \lambda$.

We obtain $ak + (v - 1 - a)\lambda = k^2$. Recall that $(v - 1)\lambda = k^2 - k$, so

$$a(k - \lambda) = k.$$

Now let B' be a block with $\omega \in B'$. Set $B = C = B' \setminus \{\omega\}$. Then $|B \cap B^g| = k - 1$ or $\lambda - 1$. Let b be the frequency of the first case. As above we get $b(k - 1) + (v - 1 - b)(\lambda - 1) = (k - 1)^2$, which simplifies to

$$b(k - \lambda) = v - k.$$

We obtain:

$$(k - \lambda)^2 \text{ divides } k(v - k), \text{ and } k - \lambda \text{ divides } k + (v - k) = v.$$

On the other hand, the basic relation $(v - 1)\lambda = k^2 - k$ is equivalent to $k(v - k) = (v - 1)(k - \lambda)$, so $k - \lambda$ divides $v - 1$. Therefore $k - \lambda = 1$, hence $k = v - 1$ and we have the trivial design, contrary to our assumption. \square

4. REMARKS ON M_{24}

In the last section, we sketch a computer based proof showing that (1) has an integer solution for $G = M_{24}$ in its permutation representation on $\Omega^{(2)}$ with $\Omega = \{1, \dots, 24\}$. As the tedious proofs of Lemmas 9, 10 and Theorem 11 are not directly related to the main goal of this paper, we omit them and will give them in a separate paper.

For a subgroup $H \leq G$, we consider the following system (2) of linear equations:

Let $\Omega_1, \Omega_2, \dots, \Omega_r$ be the orbits of H on $\Omega \times \Omega$, and T be a set of representatives for the action of H on G by conjugation. For $i = 1, 2, \dots, r$ and $g \in G$ set

$$a_i(g) = |\{(\omega_1, \omega_2) \in \Omega_i \mid \omega_1^g = \omega_2\}|$$

and consider the system of r linear equations in the variables x_g , $g \in T$:

$$(2) \quad \sum_{g \in T} x_g a_i(g) = |\Omega_i|, \quad i = 1, 2, \dots, r.$$

The system (1) is the same as the system (2) with $H = 1$. Furthermore, note that $a_i(g)$ depends only on the H -class of g , so the system of equations does not depend on the chosen system T of representatives.

Lemma 9. *Let $U \leq V \leq G$ be subgroups of G . If (2) has an integral solution for $H = U$, then (2) has an integral solution for $H = V$.*

Lemma 10. *Let $p^m > 1$ be a power of a prime p , and $R = \mathbb{Z}/p^m\mathbb{Z}$. Suppose that (2) has a solution in R for some p' -subgroup H of G . Then also (1) is solvable over R .*

The proof of Lemma 10 only uses that $|H|$ is a unit in R . So if (2) has a rational solution for some $H \leq G$, then (1) has a rational solution too. So the rational solubility of (1) can be decided by the rational solubility of (2) for $H = G$, which gives a very weak condition.

A useful criterion to decide whether (1) has an integral solution is

Theorem 11. *The following are equivalent:*

- (i) *The system (1) has an integral solution.*
- (ii) *For each prime divisor p of $|G|$, the system (2) has an integral solution for some p' -subgroup H of G .*

In order to apply this theorem to the action of $G = M_{24}$ on $\Omega^{(2)}$, we first choose a Sylow 2-subgroup H of G . So H is a p' -subgroup of G for each odd prime p . The number of H -orbits on G is 241871. So the number of unknowns is reduced by a factor $|G|/241871 = 1012.2\dots$. The number of equations is 603. In order to solve this system, one can pick about 270 variables at random, and set the remaining ones to 0. Experiments with the computer algebra system Magma [10] show that this system usually has an integral solution.

It remains to take a $2'$ -subgroup of G . For this we let H be the normalizer of a Sylow 23 -subgroup. Then $|H| = 253$. This reduces the number of unknowns from $|G| = 244823040$ by a factor of about 253 to 967692. Here, picking 520 unknowns at random usually gives an integral solution.

In both cases, the running time is a few minutes.

There are several modifications of this method. In (1) it suffices to consider the sum over the fixed-point-free elements and 1, and likewise in (2) (and the lemmas and the theorem), it suffices to consider 1 together with the H -orbits on fixed-point-free elements. However, even under this assumption, (1) still has an integral solution. To do so, one simply sets $x_1 = 1$ and randomly picks the variables x_g for fixed-point-free elements g from T .

Also, Theorem 11 and Lemma 9 remain true if we replace ‘integral’ by ‘non-negative integral’. So we are faced with an integer linear programming problem. Experiments have shown that (2) has a non-negative integral solution for each of the 29 subgroups H of $G = M_{24}$ with $[G : H] \leq 26565$.

REFERENCES

- [1] A. E. Brouwer, A. M. Cohen, A. Neumaier. Distance-regular Graphs, vol. 18 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*, Springer-Verlag, Berlin (1989).
- [2] P. Dembowski. Finite geometries. Springer-Verlag, Berlin-New York, 1968.
- [3] P. Frankl and M. Deza. On the maximum number of permutations with given maximal or minimal distance, *J. Combin. Theory Ser. A*, Vol. 22 (1977) pp. 352–360.
- [4] GAP GROUP. GAP — Groups, Algorithms, and Programming. University of St Andrews and RWTH Aachen, 2002, Version 4r3.
- [5] T. Grundhöfer. The groups of projectivities of finite projective and affine planes. Eleventh British Combinatorial Conference (London, 1987). *Ars Combin.* 25 (1988), A, 269–275.
- [6] T. Grundhöfer and P. Müller. Sharply 2-transitive sets of permutations and groups of affine projectivities. *Beiträge zur Algebra und Geometrie* 50(1) (2009), 143–154.
- [7] M. E. O’Nan. Sharply 2-transitive sets of permutations. In *Proc. Rutgers group theory year, 1983-1984* (New Brunswick, N.J., 1983-1984), pages 63–67. Cambridge Univ. Press, 1985.
- [8] J. Quistorff. A survey on packing and covering problems in the Hamming permutation space. *Electron. J. Combin.* 13 (2006), no. 1, Article 1, 13 pp. (electronic).
- [9] H. Tarnanen. Upper Bounds on Permutation Codes via Linear Programming. *Europ. J. Combinatorics* (1999) 20, 101–114.
- [10] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

E-mail address: peter.mueller@mathematik.uni-wuerzburg.de

E-mail address: nagy@math.u-szeged.hu

INSTITUT FÜR MATHEMATIK, UNIVERSITÄT WÜRZBURG, AM HUBLAND, D-97074 WÜRZBURG, GERMANY

BOLYAI INSTITUTE, UNIVERSITY OF SZEGED, ARADI VÉRTANÚK TERE 1, H-6720 SZEGED, HUNGARY